PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 5 :		(11) Internationale Veröffentlichungsnummer: WO 93/21711
H04L 9/00	A1	(43) Internationales Veröffentlichungsdatum: 28. Oktober 1993 (28.10.93)

(21) Internationales Aktenzeichen: PCT/DE93/00246

(22) Internationales Anmeldedatum: 17. März 1993 (17.03.93)

(30) Prioritätsdaten:
P 42 11 989.8 9. April 1992 (09.04.92) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US):* SIEMENS AKTIENGESELLSCHAFT [DE/DE]; Wittelsbacherplatz 2, D-8000 München 2 (DE). SIEMENS NIXDORF INFORMATIONSSYSTEME AKTIENGESELLSCHAFT: Fürstenallee 7 [DE/DE]; D-4790 Paderborn (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US) :* HOFFMANN, Gerhard [DE/DE]; Gozbertstraße 8, D-8000 München 90 (DE). LUKAS, Klaus [DE/DE]; Blaufärberstraße 6, D-8070 Ingolstadt (DE). LECHNER, Stephan [DE/DE]; Putzbrunnerstraße 1, D-8000 München 83 (DE). STEINER, Ferdinand [DE/DE]; Kaulbachstraße 42, D-8000 München 22 (DE). BAUMGÄRTNER, Helmut [DE/DE]; Arzbergerstraße 9a, D-8000 München 90 (DE). LÖHMANN, Ekkehard [DE/DE]; Humbroichweg 13, D-5300 Bonn (DE). LECLERC, Matthias [DE/DE]; Schwarzbergstraße 52, D-6000 Frankfurt 1 (DE).

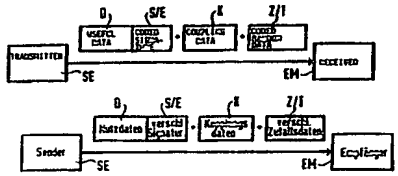
(81) Bestimmungsstaaten: US, europäisches Patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: PROCESS FOR DETECTING UNAUTHORISED REINJECTION OF DATA SENT BY A TRANSMITTER TO A RECEIVER

(54) Bezeichnung: VERFAHREN ZUM ERKENNEN EINER UNBERECHTIGTEN WIEDEREINSPIELUNG BELIEBIGER VON EINEM SENDER ZU EINEM EMPFÄNGER ÜBERTRAGENER DATEN

(57) Abstract



The process is designed to discover whether the data sent from the transmitter (SE) to the receiver (EM) have been tapped and subsequently fed back in and/or altered without authority. To this end the signature (S) allocated to the useful data (D) is symmetrically coded using a combination of coupling data (K) characterising the coupling between the transmitter and the receiver and random data (Z) provided by a random generator. The coupling data are transmitted uncoded, while the random data are coded. It is possible at the reception end to detect whether the message transmitted has been tapped and fed back into the system if the coupling data are incorrect. An alteration to the transmitted message can be detected in that the code used to encode the signature, which is obtained from a combination of coupling data and random data with the aid of a one-way function, does not correspond to the code obtained at the receiver during decoding and thus the decoding of the encoded signature gives an incorrect result. This is recognised on verification of the signature.

(57) Zusammenfassung

Mit dem Verfahren soll festgestellt werden, ob die vom Sender (SE) zum Empfänger (EM) übertragenen Daten abgehört und später eingespielt worden sind und/oder unzulässig geändert worden sind. Dazu wird die den Nutzdaten (D) zugeordnete Signatur (S) symmetrisch unter Verwendung einer Kombination von die Kopplung zwischen Sender und Empfänger kennzeichnenden Kopplungsdaten (K) und von einem Zufallsgenerator erzeugten Zufallsdaten (Z) verschlüsselt. Die Kopplungsdaten werden im Klartext übertragen, die Zufallsdaten verschlüsselt. Auf der Empfängerseite kann festgestellt werden, ob die übertragene Nachricht abgehört und später wieder eingespielt worden ist, wenn die Kopplungsdaten unzulässig sind. Eine Änderung der übertragenen Nachricht kann dadurch festgestellt werden, daß der zur Verschlüsselung der Signatur verwendete Schlüssel, der aus der Kombination von Kopplungsdaten und Zufallsdaten mit Hilfe einer Einwegfunktion gewonnenen worden ist, nicht dem bei der Entschlüsselung beim Empfänger gewonnen Schlüssel entspricht und somit die Entschlüsselung der verschlüsselten Signatur zu einem falschen Ergebnis führt. Dies wird beim Verifizieren der Signatur erkannt.

LEDIGLICH ZUR INFORMATION

Code, die zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AT	Österreich			MR	Mauritanien
AU	Australien	FR	Frankreich	MW	Malawi
BB	Barbados	GA	Gabon	NL	Niederlande
BE	Belgien	GB	Vereinigtes Königreich	NO	Norwegen
BF	Burkina Faso	GN	Guinea	NZ	Neuseeland
BG	Bulgarien	GR	Griechenland	PL	Polen
BJ	Benin	HU	Ungarn	PT	Portugal
BR	Brasilien	IE	Irland	RO	Rumänien
CA	Kanada	IT	Italien	RU	Russische Föderation
CF	Zentrale Afrikanische Republik	JP	Japan	SD	Sudan
CG	Kongo	KP	Demokratische Volksrepublik Korea	SE	Schweden
CH	Schweiz	KR	Republik Korea	SK	Slowakischen Republik
CI	Côte d'Ivoire	KZ	Kasachstan	SN	Senegal
CM	Kamerun	LI	Liechtenstein	SU	Soviet Union
CS	Tschechoslowakei	LK	Sri Lanka	TD	Tschad
CZ	Tschechischen Republik	LU	Luxemburg	TG	Togo
DE	Deutschland	MC	Monaco	UA	Ukraine
DK	Dänemark	MG	Madagaskar	US	Vereinigte Staaten von Amerika
ES	Spanien	ML	Mali	VN	Vietnam
FI	Finnland	MN	Mongolei		

Verfahren zum Erkennen einer unberechtigten Wiedereinspielung beliebiger von einem Sender zu einem Empfänger übertragener Daten

Es ist bekannt, die von einem Sender zu einem Empfänger zu übertragenden Daten dadurch gegen unberechtigten Angriff zu schützen, daß die Daten verschlüsselt werden. Zum Beispiel ergibt sich aus H. Sedlak, U. Golze, Ein Public-Key-Code Kryptographie-Prozessor, Informationstechnik it, 28. Jahrgang, Heft 3/1986, Seite 157, 158 eine einführende Schilderung der Möglichkeiten der Sicherung von Daten, die von einem Sender zu einem Empfänger zu übertragen sind. Dabei kann sowohl der Sender als auch der Empfänger ein Rechner sein. Die Verschlüsselung oder Sicherung soll dazu führen, daß die Authenzität des Absenders sowie ein Manipulationsschutz der Nachricht oder der Daten erreicht wird. Dazu können die Nachrichten, die zu übertragen sind, verschlüsselt werden, z.B. nach einem asymmetrischen oder symmetrischen Verschlüsselungsverfahren. Asymmetrisch heißt dabei, daß zum Ver- und Entschlüsseln zwei verschiedene Schlüssel verwendet werden. Ebenso ist es möglich, sowohl bei Empfänger als auch bei Sender denselben Schlüssel zu verwenden, womit eine symmetrische Verschlüsselung erreicht wird. Bei den asymmetrischen Verfahren ist es möglich, daß ein Schlüssel sich nicht ohne Zusatzinformationen aus dem anderen Schlüssel berechnen läßt. Deshalb kann einer der beiden Schlüssel veröffentlicht werden. Dieses Verfahren wird auch Public-Key-Verfahren genannt.

Die zu übertragende Nachricht besteht gewöhnlich aus Nutzdaten und einer aus den Nutzdaten entwickelten Signatur.

Die Signatur ist ein mit dem Absenderschlüssel verschlüsselter Extrakt der Nutzdaten. Mit Hilfe des Empfängerschlüssels kann dann festgestellt werden, ob die entschlüsselte Signatur aus den übertragenen Nutzdaten entwickelbar ist. Figur 1 zeigt dieses Prinzip. Die Nutzdaten D werden beim Sender SE vor dem Versenden mit einem Signierschlüssel digital unterschrieben. Es ergibt sich die Signatur S. Die Nutzdaten werden daraufhin zusammen mit der Signatur an den Empfänger EM übertragen. Der Empfänger EM überprüft mit Hilfe des korrespondierenden Verifikationsschlüssels die Integrität der aus Nutzdaten und Signatur bestehenden Nachricht und die Authentizität der Unterschrift.

Ein potentieller Angreifer kann den Datenverkehr abhören und die abgehörten Daten samt Signatur beim Empfänger oder bei einer anderen Stelle, die im Besitz des Verifikationsschlüssels ist, wieder einspielen. Der Empfänger hat keine Möglichkeit, anhand der Signatur zu erkennen, ob diese original sind oder ob es um eine Wiedereinspielung handelt.

Das der Erfindung zugrundeliegende Problem besteht darin, ein Verfahren anzugeben, bei dem der Empfänger erkennen kann, ob die empfangenen Daten direkt vom Sender übertragene Daten oder von einem Angreifer unberechtigt eingespielte Daten sind. Dieses Problem wird gemäß den Merkmalen des Patentanspruches 1 gelöst.

Das erfindungsgemäße Verfahren beruht im wesentlichen auf einer symmetrischen Verschlüsselung der Signatur. Durch diese Verschlüsselung kann eine fälschungssichere Kopplung der Signatur an einen bestimmten Datenaustausch zwischen Sender und Empfänger erreicht werden.

Dazu ist es vorteilhaft, in den bei der Verschlüsselung der Signatur verwendeten Schlüssel sog. Kopplungsdaten

eingehen zu lassen, anhand derer ein unberechtigtes Wiedereinspielen erkannt werden kann. Solche Kopplungsdaten können z.B. eine Kennzeichnung des Empfängers oder die Zeit der Datenübertragung sein. Die Kopplungsdaten können dem Empfänger im Klartext zur Überprüfung zusätzlich zu den Nutzdaten und der verschlüsselten Signatur übermittelt werden.

Um weiterhin eine unberechtigte Rückgewinnung der Originalsignatur zu verhindern, gehen in den Schlüssel zur Verschlüsselung der Signatur zusätzlich vom Sender erzeugte Zufallsdaten ein. Diese Zufallsdaten können ebenfalls an den Empfänger übertragen werden und zwar verschlüsselt. Zur Verschlüsselung der Zufallsdaten kann ein sog. Transferschlüssel verwendet werden, der sowohl ein symmetrischer als auch ein asymmetrischer Schlüssel sein kann.

Beim Sender kann ein Zufallszahlengenerator zur Verfügung stehen. Die Verschlüsselung der Signatur kann unter Verwendung einer für Sender und Empfänger gemeinsamen Einwegfunktion erfolgen, die auch öffentlich bekannt sein kann. Schließlich teilen sich Sender und Empfänger einen geheimen Schlüssel bei Einsatz symmetrischer Verschlüsselungsverfahren bzw. ein Schlüsselpaar bei Einsatz asymmetrischer Krypto- oder Verschlüsselungsverfahren.

Weiterbildungen der Erfindung ergeben sich aus den Unteransprüchen.

Anhand eines Ausführungsbeispieles, das in den Figuren dargestellt ist, wird die Erfindung weiter erläutert.
Es zeigen
Figur 2 ein Prinzipbild der von Sender zu Empfänger übertragenen Nachricht,

Figur 3 ein Schema des senderseitigen Schutzalgorithmus,
Figur 4 ein Schema des empfängerseitigen Schutzalgorithmus.

Ausgehend von Figur 1 und 2 sollen Nutzdaten D von einem Sender SE zu einem Empfänger EM übertragen werden. Auf der Senderseite stehen folgende Daten zur Verfügung: Nutzdaten D und die dazugehörige Signatur S sowie ein Transferschlüssel T, der eine vertrauliche Übermittlung der Zufallsdaten Z ermöglicht. Die Übertragung kann z.B. über eine Übertragungsleitung erfolgen. Um die Übertragung der Nutzdaten zu sichern, wird eine Signatur S verwendet, die zur verschlüsselten Signatur S/E umgewandelt worden ist. Zusätzlich zu den Nutzdaten D und der verschlüsselten Signatur S/E können Kopplungsdaten K und verschlüsselte Zufallsdaten Z/T zum Empfänger EM übertragen werden. Die vom Sender SE zum Empfänger EM übertragene Nachricht besteht somit aus Nutzdaten D, verschlüsselter Signatur S/E, Kopplungsdaten K und verschlüsselten Zufallsdaten Z/T.

Nach Figur 3 wird die vom Sender SE zum Empfänger EM zu übertragende Nachricht auf folgende Weise erzeugt:

1. Zunächst werden Zufallsdaten Z von einem Zufallsdatengenerator beim Sender erzeugt.
2. Weiterhin werden Kopplungsdaten K festgelegt.
3. Aus einer Kombination von Zufallsdaten Z und Kopplungsdaten K wird durch Einwegverschlüsselung ein symmetrischer Schlüssel E erzeugt. Die dazu verwendete Einwegfunktion kann öffentlich bekannt sein.
4. Mit Hilfe des Schlüssels E wird die Signatur S symmetrisch verschlüsselt und die verschlüsselte Signatur S/E erzeugt.
5. Weiterhin werden mit Hilfe eines Transferschlüssels T die Zufallsdaten Z zu verschlüsselten Zufallsdaten Z/T verschlüsselt.
6. Anschließend kann die Nachricht vom Sender zum Empfän-

ger übertragen werden, bestehend aus Nutzdaten D, verschlüsselter Signatur S/E, Kopplungsdaten K und verschlüsselten Zufallsdaten Z/T.

Nach Figur 4 stehen auf der Empfängerseite EM somit eine Nachricht zur Verfügung, die aus Nutzdaten D, verschlüsselter Signatur S/E, Kopplungsdaten K, verschlüsselten Zufallsdaten Z/T besteht, zusätzlich ist ein korrespondierender Transferschlüssel T gegeben.

Zur Überprüfung der übertragenen Nachricht werden nun folgende Schritte durchgeführt:

1. Die Kopplungsdaten K werden auf Plausibilität untersucht. Ergeben sich aus der Überprüfung Unstimmigkeiten, so wird die Nachricht zurückgewiesen. Bei der Plausibilitätsprüfung wird also geprüft, ob die Kopplungsdaten richtig sein können. Beispiele von Kopplungsdaten werden weiter unten behandelt.
2. Die Zufallsdaten Z werden durch Entschlüsselung der verschlüsselten Zufallsdaten Z/T mit Hilfe des Transferschlüssels T zurückgewonnen.
3. Aus den berechneten Zufallsdaten Z und den erhaltenen Kopplungsdaten K wird unter Verwendung einer Einwegverschlüsselung der verwendete symmetrische Schlüssel E bestimmt.
4. Durch Entschlüsselung der verschlüsselten Signatur S/E mit Hilfe des berechneten Schlüssels E wird die Signatur S zurückgewonnen.
5. Die Signatur S wird überprüft. Ergeben sich aus der Prüfung Fehler, so wird die Nachricht zurückgewiesen.

Die Kopplungsdaten K und die Zufallsdaten Z/T können nicht unerkannt gefälscht werden. Eine Fälschung wird spätestens bei der Überprüfung der Signatur durch den Empfänger EM bemerkt. Eine Modifikation der Kopplungsdaten K und der

verschlüsselten Zufallsdaten Z/T führt nämlich beim Empfänger zu einem verfälschten symmetrischen Schlüssel E; die Entschlüsselung der verschlüsselten Signatur S/E mit dem verfälschten Schlüssel E' führt zu einer ungültigen Signatur S'. Dies wird schließlich beim Verifizieren der Signatur S' erkannt und als Fälschung zurückgewiesen.

Ein Wiedereinspielen der Nachricht kann anhand der Kopplungsdaten K vom Empfänger EM erkannt werden. Welche speziellen Wiedereinspielangriffe abgewehrt werden können, hängt von der Wahl der Kopplungsdaten ab. Anhand einiger Beispiele soll erläutert werden, wie sich bestimmte Einträge in die Kopplungsdaten auswirken.

Wenn die Kopplungsdaten aus einem leeren Eintrag bestehen, besteht eine implizite Kopplung der mit der Signatur versehenen Nutzdaten an die Besitzer des Transferschlüssels. Die abgehörten Daten können nicht unerkannt bei Systemen eingespielt werden, die nicht im Besitz des Transferschlüssels sind.

Die Kopplungsdaten können aus einem Eintrag des Empfängernamens bestehen. Dann kann der Empfänger überprüfen, ob die Nachricht wirklich für ihn bestimmt war oder ob die Nachricht ursprünglich an einen anderen Adressaten gerichtet war, abgehört und wieder eingespielt worden ist. Der Empfänger kann jedoch nicht überprüfen, ob die Nachricht schon früher einmal an ihn gesendet wurde.

Die Kopplungsdaten können aus einem Eintrag der Sendezeit bestehen. Jeder der Empfänger kann dann überprüfen, ob die Nachricht aktuell ist oder ob es sich um eine Wiedereinspielung älteren Datums handelt. Allerdings könnte der Datenverkehr abgehört und quasi zeitgleich an anderer Stelle wieder eingespielt werden.

Eine beliebige Kombination von verschiedenen Einträgen in die Kopplungsdaten ist möglich. Werden mehrere Einträge in den Kopplungsdaten kombiniert, so müssen sämtliche Einträge hinsichtlich ihrer Plausibilität überprüft werden. Nur wenn alle Prüfungen positiv ausfallen, wird die Nachricht anerkannt. Je mehr Informationen in den Kopplungsdaten mitgeschickt werden, desto stärker ist die Kopplung der unterschriebenen Daten an einen ganz bestimmten Auftrag.

Durch die Verwendung von Zufallsdaten Z, die in den Schlüssel E eingehen, kann festgestellt werden, ob die Nachricht auf dem Weg vom Sender zum Empfänger geändert worden ist. Da die Zufallsdaten verschlüsselt übertragen werden und bei der Bildung des Schlüssels E sowohl die Zufallsdaten als auch die Kopplungsdaten eingehen, kann jede Änderung der übertragenen Nachricht festgestellt werden.

Als Transferschlüssel kann sowohl ein symmetrischer als auch ein asymmetrischer Schlüssel verwendet werden. Für den Fall, daß beide Kommunikationspartner gegenseitig signierte Daten austauschen und dabei ein Public-Key-Verfahren benutzen, können die verwendeten Signier- und Verifikationsschlüssel auch als Transportschlüssel verwendet werden. Beim Verschlüsseln der Zufallsdaten auf der Senderseite dient der öffentliche Schlüssel des Empfängers als Transferschlüssel. Beim Entschlüsseln der Zufallsdaten auf der Empfängerseite dient der private Schlüssel des Empfängers als Transferschlüssel.

Das erfindungsgemäße Verfahren läßt sich auch auf Prüfsummen von Daten anwenden. Anstatt der Signatur wird die entsprechende Prüfsumme symmetrisch verschlüsselt. Die einzelnen Verfahrensschritte beim Verschlüsseln und Entschlüsseln der Prüfsumme bleiben unverändert.

Patentansprüche

1. Verfahren zum Erkennen einer unberechtigten Wiedereinspielung beliebiger von einem Sender (SE) zu einem Empfänger (EM) übertragener Daten,
-bei dem die Daten aus Nutzdaten (D) und einer aus den Nutzdaten entwickelten Signatur (S) bestehen,
-bei dem die Signatur (S) symmetrisch verschlüsselt wird und der dazu verwendete Schlüssel (E) von die Übertragung zwischen Sender und Empfänger bezeichnenden Kopplungsdaten (K) abhängig ist.

2. Verfahren nach Anspruch 1, bei dem die Kopplungsdaten (K) von der Zeit der Übertragung der Daten und/oder dem Empfänger abhängig sind.

3. Verfahren nach Anspruch 1 oder 2, bei dem die Kopplungsdaten (K) im Klartext an den Empfänger (EM) übertragen werden.

4. Verfahren nach einem der Ansprüche 1 bis 3, bei dem der Schlüssel (E) beim Sender (SE) zusätzlich von Zufallsdaten oder Pseudozufallsdaten (Z) beeinflußt wird.

5. Verfahren nach Anspruch 4, bei dem die Zufallsdaten (Z) mit einem Transferschlüssel (T) verschlüsselt an den Empfänger (EM) übertragen werden.

6. Verfahren nach Anspruch 5,
-bei dem die Zufallsdaten (Z) erzeugt werden,
- bei dem die Kopplungsdaten (K) festgelegt werden,
- bei dem ein symmetrischer Schlüssel (E) durch Einwegverschlüsselung der Kombination der Zufallsdaten und der Kopplungsdaten erzeugt wird,
- bei dem die Signatur (S) mit Hilfe des Schlüssels (E) verschlüsselt wird,

- bei dem die Zufallsdaten (Z) mit dem Transferschlüssel (T) verschlüsselt werden,
- bei dem eine Nachricht bestehend aus den Nutzdaten (D), der verschlüsselten Signatur (S/E) den Kopplungsdaten (K) und den verschlüsselten Zufallsdaten (Z/T) versendet wird.

7. Verfahren nach Anspruch 6, bei dem auf der Empfängerseite die Kopplungsdaten (K) überprüft werden und bei Unstimmigkeit die Nachricht zurückgewiesen wird,
- bei dem die Zufallsdaten (Z) durch Entschlüsselung der erhaltenen verschlüsselten Zufallsdaten (Z/T) mit dem Transferschlüssel (T) zurückgewonnen werden,
- bei dem der symmetrische Schlüssel (E) durch Einwegverschlüsselung der Kombination aus den berechneten Zufallsdaten (Z) und erhaltenen Kopplungsdaten (K) bestimmt wird,
- bei dem die Signatur (S) durch Entschlüsselung der verschlüsselten Signatur (S/E) mit Hilfe des berechneten Schlüssels (E) zurückgewonnen wird,
- bei dem die Signatur (S) überprüft wird und bei Feststellung von Fehlern die Nachricht zurückgewiesen wird.

8. Verfahren nach einem der Ansprüche 5 bis 7,bei dem als Transferschlüssel (T) ein symmetrischer Schlüssel verwendet wird.

9. Verfahren nach einem der Ansprüche 5 bis 7, bei dem als Transferschlüssel (T) ein asymmetrischer Schlüssel verwendet wird, wobei nach dem Public-Key-Verfahren vorgegangen wird.

10. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die Signatur durch eine Prüfsumme der Nutzdaten ersetzt wird.

11. Verfahren nach einem der vorhergehenden Ansprüche, bei dem die Nutzdaten durch Protokolldaten oder einer Kombination von Protokoll- und Nutzdaten ersetzt wird.

FIG 1

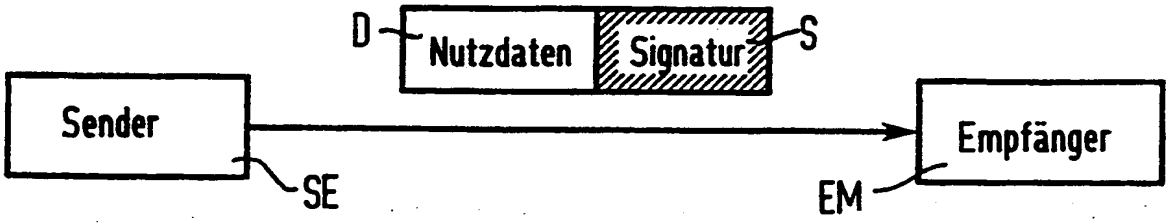


FIG 2

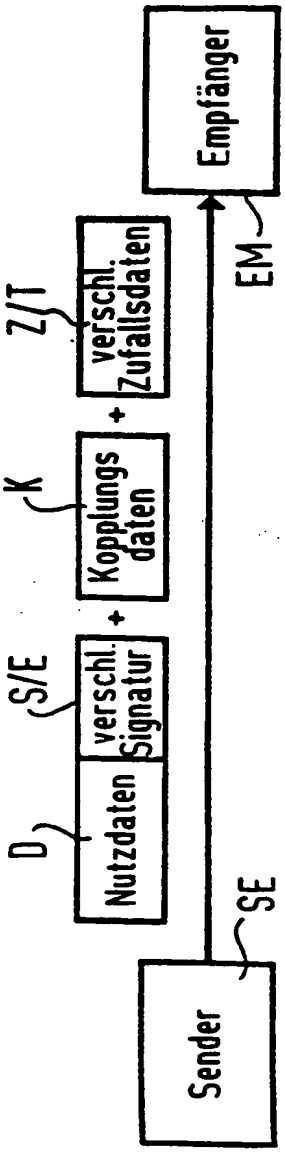


FIG 3

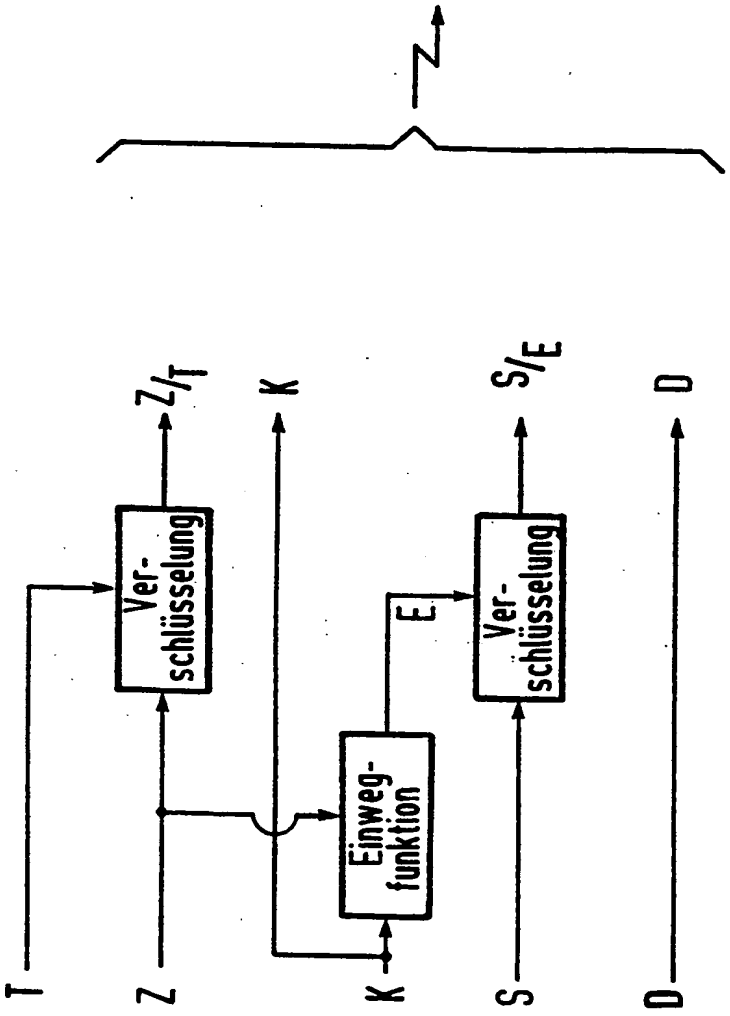
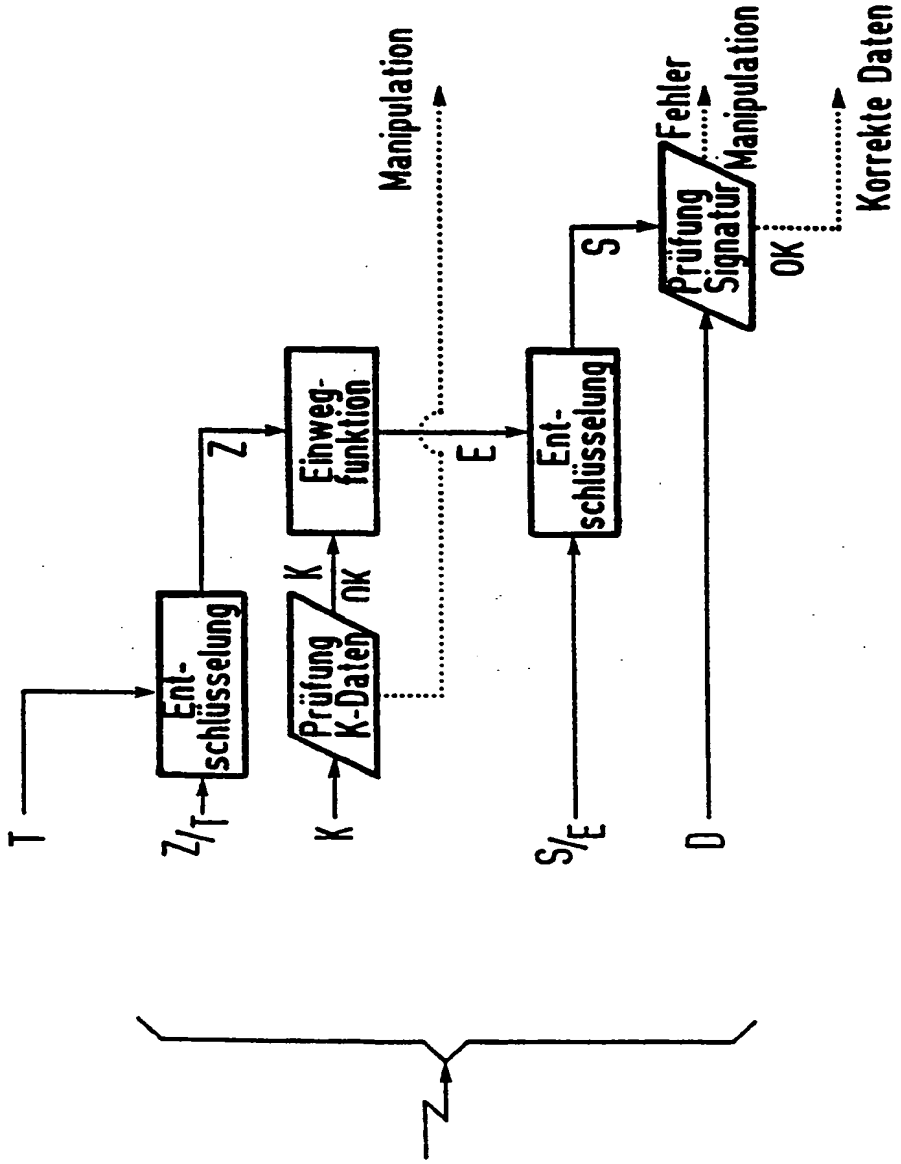

Z
Z/T
K
S/E
D
Ver-
schlüsselung
E
Ver-
schlüsselung
Einweg-
funktion
T
Z
K
S
D

FIG 4


T
Z/T
Entschlüsselung
Z
Einwegfunktion
K
Prüfung K-Daten
nK
Manipulation
E
Entschlüsselung
S/E
S
Prüfung Signatur
Fehler
Manipulation
OK
Korrekte Daten
D
Z

INTERNATIONAL SEARCH REPORT

International application No.
PCT/DE93/00246

A. CLASSIFICATION OF SUBJECT MATTER

Int. Cl.^{5} : H04L 9/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

Int. Cl.^{5} : H04L, H04K

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

ORBIT : WPAT

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US, A, 4578530 (HOWARD M. ZEIDLER) 25 March 1986 (25.03.86), column 3, line 6 - column 5, line 11; column 8, line 4 - column 9, line 17; column 10, lines 17-28, figure 14, abstract	1-5,8-11
A	---	6-7
A	EP, A2, 0197392 (INTERNATIONAL BUSINESS MACHINES CORPORATION), 15 October 1986 (15.10.86), column 1, lines 29-51; column 2, line 24 - column 3, line 12	1

A	EP, A2, 0117907 (GABE GELDAUSGABEAUTOMATEN-SERVICE GESELLSCHAFT M.B.H.) 12 September 1984 (12.09.84), page 2, line 27 - page 3, line 26	1-2

A	US, A, 4853962 (ROBERT T. BROCKMAN), 1 August 1989 (01.08.89), column 1, line 56 - column 2, line 15, figure 7, abstract	2

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 June 1993 (14.06.93)	8 July 1993 (08.07.93)
Name and mailing address of the ISA/	**Authorized officer**
European Patent Office	
Facsimile No.	**Telephone No.**

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/DE93/00246

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 4281215 (MARTIN M. ATALLA), 28 July 1981 (28.07.81), column 3, line 31 - column 4, line 11, figures 3A-3B, abstract	6,7

SA 71277

INTERNATIONAL SEARCH REPORT

Information on patent family members

28/05/93

International application No.
PCT/DE 93/00246

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US-A- 4578530	25/03/86	EP-A,B- 0068805	05/01/83
		JP-C- 1593570	14/12/90
		JP-B- 2018512	25/04/90
		JP-A- 58004476	11/01/83
		US-A- 4423287	27/12/83
EP-A2- 0197392	15/10/86	CA-A- 1249865	07/02/89
		DE-A- 3682309	12/12/91
		JP-C- 1694867	17/09/92
		JP-B- 3063261	30/09/91
		JP-A- 61237546	22/10/86
		US-A- 4649233	10/03/87
EP-A2- 0117907	12/09/84	AT-B- 388472	26/06/89
		DE-A- 3377431	25/08/88
US-A- 4853962	01/08/89	NONE	
US-A- 4281215	28/07/81	CA-A- 1149484	05/07/83
		CA-A- 1159124	20/12/83
		CA-A- 1159920	03/01/84
		CH-A- 646558	30/11/84
		DE-A,C- 2916454	15/11/79
		FR-A,B- 2425114	30/11/79
		GB-A,B- 2020513	14/11/79
		GB-A,B- 2047506	26/11/80
		GB-A,B- 2099195	01/12/82
		JP-A- 54148402	20/11/79
		JP-A- 62283742	09/12/87
		US-A- 4268715	19/05/81

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 93/00246

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPC5: H04L 9/00
Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPC5: H04L, H04K

Recherte, aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

ORBIT: WPAT

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US, A, 4578530 (HOWARD M. ZEIDLER), 25 März 1986 (25.03.86), Spalte 3, Zeile 6 - Spalte 5, Zeile 11; Spalte 8, Zeile 4 - Spalte 9, Zeile 17; Spalte 10, Zeile 17 - Zeile 28, Figur 14, Zusammenfassung	1-5,8-11
A	--	6-7
A	EP, A2, 0197392 (INTERNATIONAL BUSINESS MACHINES CORPORATION), 15 Oktober 1986 (15.10.86), Spalte 1, Zeile 29 - Zeile 51; Spalte 2, Zeile 24 - Spalte 3, Zeile 12	1
	--	
A	EP, A2, 0117907 (GABE GELDAUSGABEAUTOMATEN-SERVICE GESELLSCHAFT M.B.H.), 12 September 1984 (12.09.84), Seite 2, Zeile 27 - Seite 3, Zeile 26	1-2
	--	

[X] Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen.

[X] Siehe Anhang Patentfamilie.

* Besondere Kategorien von angegebenen Veröffentlichungen:

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung: die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung: die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachman naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche	Absendedatum des internationalen Recherchenberichts
14 Juni 1993	08. 07. 93

Name und Postanschrift der Internationalen Recherchenbehörde	Bevollmächtigter Bediensteter
Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax (+31-70) 340-3016	Magnus Stiebe

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/DE 93/00246

C (Fortsetzung). ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	US, A, 4853962 (ROBERT T. BROCKMAN), 1 August 1989 (01.08.89), Spalte 1, Zeile 56 - Spalte 2, Zeile 15, Figur 7, Zusammenfassung --	2
A	US, A, 4281215 (MARTIN M. ATALLA), 28 Juli 1981 (28.07.81), Spalte 3, Zeile 31 - Spalte 4, Zeile 11, Figuren 3A-3B, Zusammenfassung -- --------	6,7

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören 28/05/93

Internationales Aktenzeichen PCT/DE 93/00246

Im Recherchenbericht angefurtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US-A- 4578530	25/03/86	EP-A,B- 0068805	05/01/83
		JP-C- 1593570	14/12/90
		JP-B- 2018512	25/04/90
		JP-A- 58004476	11/01/83
		US-A- 4423287	27/12/83
EP-A2- 0197392	15/10/86	CA-A- 1249865	07/02/89
		DE-A- 3682309	12/12/91
		JP-C- 1694867	17/09/92
		JP-B- 3063261	30/09/91
		JP-A- 61237546	22/10/86
		US-A- 4649233	10/03/87
EP-A2- 0117907	12/09/84	AT-B- 388472	26/06/89
		DE-A- 3377431	25/08/88
US-A- 4853962	01/08/89	KEINE	
US-A- 4281215	28/07/81	CA-A- 1149484	05/07/83
		CA-A- 1159124	20/12/83
		CA-A- 1159920	03/01/84
		CH-A- 646558	30/11/84
		DE-A,C- 2916454	15/11/79
		FR-A,B- 2425114	30/11/79
		GB-A,B- 2020513	14/11/79
		GB-A,B- 2047506	26/11/80
		GB-A,B- 2099195	01/12/82
		JP-A- 54148402	20/11/79
		JP-A- 62283742	09/12/87
		US-A- 4268715	19/05/81